PathBuildRoot

The output buffer must be large enough to hold four characters

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3531 bytes

| Attack Category | Malicious Input | | | | |
|---|--|---|---|----------|--|
| | Path spoofing | Path spoofing or confusion problem | | | |
| Vulnerability Category | Buffer Over | Buffer Overflow | | | |
| | Unconditional | | | | |
| Software Context | File Path Ma | File Path Management | | | |
| Location | • shlwapi.h | • shlwapi.h | | | |
| Description | The output buffer for the PathBuildRoot() function must be large enough to hold four characters. | | | | |
| | PathBuildRoot() creates a root path from a given drive number. | | | | |
| | to hold the return an integer (e.g. 3) path of that drive | The destination string buffer must be long enough to hold the return root string. The routine takes an integer (e.g. 3) and fills in a string for the root path of that drive number (e.g. "D:\"). Therefore, the buffer must receive exactly 3 characters plus a NULL character. | | | |
| APIs | Function Name | Function Name | | Comments | |
| | PathBuildRoot | | | | |
| | PathBuildRootA | | | | |
| | 11 | tW | | | |
| | PathBuildRootW | 7 | | | |
| Method of Attack | PathBuildRootW Attacker can caus variable is not at | se a buffe | | _ | |
| | Attacker can caus | se a buffe | | _ | |
| Method of Attack Exception Criteria Solutions | Attacker can caus | se a buffe | aracters : | _ | |
| Exception Criteria | Attacker can caus variable is not at Solution | se a buffe least 4 ch | n tion put szRoot, at least | Solution | |

 $^{1. \}quad http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html~(Barnum, Sean)\\$

PathBuildRoot 1

| | LPTSTR szRoot, int iDrive); | | |
|-----------------------------------|---|--|--|
| Examples of Incorrect Code | <pre>TCHAR buffer_1[3]; // buffer is too small LPTSTR lpStr1; lpStr1 = buffer_1;</pre> | | |
| | <pre>cout << "The root path for 0 is " << PathBuildRoot(lpStr1,0) << endl;</pre> | | |
| Examples of Corrected Code | <pre>TCHAR buffer_1[4]; // buffer is correctly sized LPTSTR lpStr1; lpStr1 = buffer_1;</pre> | | |
| | <pre>cout << "The root path for 0 is " << PathBuildRoot(lpStr1,0) << endl;</pre> | | |
| Source Reference | http://msdn.microsoft.com/library/default.asp? url=/library/en-us/shellcc/platform/shell/ reference/shlwapi/path/pathbuildroot.asp² | | |
| Recommended Resource | | | |
| Discriminant Set | Operating System • Windows | | |
| | Languages • C • C++ | | |

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

2 PathBuildRoot

mailto:copyright@cigital.com